The Class Equation

If \( X \) is a \( G \)-set, \( X \) is partitioned by the \( G \)-orbits. So if \( X \) is finite,
\[
|X| = \sum_{x \in X/G} |Gx|.
\]

("\( x \in X/G \)" means you should take one representative \( x \) from each orbit, and sum over the set of representatives. This is different from the notation "\( K \in X/G \)" which occurred in the proof of Burnside’s Theorem; there I was actually summing over the set of orbits.)

\( x \) is a fixed point if \( gx = x \) for all \( g \in G \). In this case, \( x \) is an orbit all by itself. Recall that \( X^G \) denotes the set of fixed points of \( X \). I can pull these one-point orbits out of the sum above to obtain
\[
|X| = |X^G| + \sum_{x \in \Sigma} |Gx|.
\]

In this case, \( \Sigma \) will denote the set of orbits which have more than one point. (I’ll call them nontrivial orbits for short.) Thus, "\( x \in \Sigma \)" means that you should take one representative \( x \) from each nontrivial orbit.

---

**Example.** Here is a set \( X \) of 9 points arranged in a square:

\[
\begin{array}{ccc}
1 & 2 & 3 \\
4 & 5 & 6 \\
7 & 8 & 9 \\
\end{array}
\]

Let the group \( D_4 \) of symmetries of the square act on \( X \). There is one fixed point: 5. There are two nontrivial orbits: \( \{1, 3, 7, 9\} \) and \( \{2, 4, 6, 8\} \). The equation above says
\[
9 = 1 + (4 + 4). \quad \square
\]

---

**Lemma.** If \( G \) is a group, \( G \) acts on itself by conjugation:
\[
g \ast x = g x g^{-1} \quad \text{for} \quad g, x \in G.
\]

**Proof.** \( 1 \ast x = 1 \cdot x \cdot 1^{-1} = x \) for all \( x \in G \). And if \( a, b, c \in G \), then
\[
(ab) \ast x = (ab)x(ab)^{-1} = abx b^{-1} a^{-1} = a(b \ast x) a^{-1} = a \ast (b \ast x).
\]

Therefore, conjugation is an action. \( \square \)

**Definition.** The orbit of an element of \( G \) under the conjugation action is called a conjugacy class.

**Remark.** I proved earlier that if \( x \) and \( y \) are two points in the same orbit, there is a \( g \in G \) such that \( g \ast x = y \). It follows that any two elements in a conjugacy class are conjugate. \( \square \)

---

**Example.** Let \( G = S_3 \). The conjugacy classes are
\[
\{\text{id}\}, \{(1 2), (1 3), (2 3)\}, \{(1 2 3), (1 3 2)\}.
\]
Definition. Let \( G \) be a group, and let \( x \in G \). The centralizer of \( x \) is
\[
C(x) = \{ g \in G \mid gxg^{-1} = x \}.
\]

Lemma. Let \( G \) act on itself by conjugation, and let \( x \in G \). Then \( G_x = C(x) \), the centralizer of \( x \).

Proof. Fix \( x \in G \). When is \( g \in G \) in \( G_x \)? \( g \in G_x \) means \( g \) fixes \( x \), i.e. \( gxg^{-1} = x \). This is equivalent to \( gx = xg \), which in turn is what it means for \( x \) to be in \( C(x) \). \( \Box \)

Corollary. Let \( G \) act on itself by conjugation, and let \( x \in G \). Then:

(a) \( |Gx| = (G:C(x)) \).

(b) The number of elements in each conjugacy class divides the order of \( G \).

Proof. For (a), recall that the order of the orbit equals the index of the isotropy group, and I just showed the the isotropy group of \( x \) is \( C(x) \). Then (b) is immediate, since \( |G| = (G:C(X))|C(x)| \), i.e. \( |G| = |Gx||C(x)| \). \( \Box \)

Corollary. Let \( G \) act on itself by conjugation. Then \( G^G = Z(G) \).

(The horrible notation \( G^G \) means the elements of \( G \) fixed under the conjugation action. I promise not to do it again.)

Proof. The orbit of a fixed point consists of the point itself, so \( |Gx| = 1 \). This is equivalent to \( (G:C(x)) = 1 \), or \( G = C(x) \). This is the same as saying that everything commutes with \( x \), i.e. \( x \in Z(G) \). \( \Box \)

I’ll apply these results to the equation
\[
|X| = |X^G| + \sum_{x \in \Sigma} |Gx|.
\]

In this case, the \( G \)-set is \( X = G \). The set of fixed points is the center: \( X^G = Z(G) \). The nontrivial orbits \( \Sigma \) consist of conjugacy classes with more than one element. The order of such a conjugacy class is \( (G:C(x)) \), where \( C(x) \) is the centralizer of \( x \). (I must take one such \( x \) for each nontrivial orbit.) Therefore,

\[
|G| = |Z(G)| + \sum_{x \in \Sigma} (G:C(x)).
\]

This is called the class equation.

Example. Let \( G = S_3 \). The center of \( S_3 \) is \( Z(S_3) = \{ \text{id} \} \), and the nontrivial conjugacy classes are
\[
\{(1 2), (1 3), (2 3)\}, \{(1 2 3), (1 3 2)\}.
\]

Take one element from each nontrivial class: say \( (1 2) \) and \( (1 2 3) \). Their centralizers are
\[
C((1 2)) = \{ \text{id}, (1 2) \} \quad \text{and} \quad C((1 2 3)) = \{ \text{id}, (1 2 3), (1 3 2) \}.
\]

Thus,
\[
|Z(S_3)| + (S_3 : C((1 2))) + (S_3 : C((1 2 3))) = 1 + 3 + 2 = 6 = |S_3|.
\]
**Example.** Consider the group \( Q = \{\pm 1, \pm i, \pm j, \pm k\} \) of quaternions. Here are the conjugacy classes:

- Central elements: \( \{1\}, \{-1\} \)
- Nontrivial conjugacy classes: \( \{i, -i\}, \{j, -j\}, \{k, -k\} \)

I found these by direct computation. For example, the conjugates of \( i \) are:

\[
\begin{align*}
1 \cdot i \cdot (-1) &= -i \\
i \cdot i \cdot (-i) &= i \\
j \cdot i \cdot (-j) &= -i \\
k \cdot i \cdot (-k) &= -i
\end{align*}
\]

Hence, \( \{i, -i\} \) is a complete conjugacy class.

In the class equation, the sum is taken over a set of representatives \( \Sigma \) for the nontrivial conjugacy classes. In this example, for instance, I could take \( \Sigma = \{i, j, k\} \) or \( \Sigma = \{-i, -j, k\} \) or \( \cdots \) — i.e. any three elements, one from each of the (nontrivial) classes \( \{i, -i\}, \{j, -j\}, \{k, -k\} \).

Finally, note that \( |Z(Q)| = 2 \), and the nontrivial classes have 2, 2, and 2 elements, respectively. The class equation says (correctly) that

\[
2 + (2 + 2 + 2) = 8. \quad \Box
\]

Before I prove the next result, I'll review some things that are apparent from the derivation of the class equation. I had \( G \) acting on itself by conjugation. Then an orbit \( Gx \) (which does not mean "\( G \) times \( x \)" in this case!) is the conjugacy class of \( x \) — i.e. the set of elements conjugate to \( x \). Assuming that \( G \) is finite, the order of the orbit equals the index of of the isotropy group, so \( |Gx| = (G : C(x)) \), where \( C(x) \) is the centralizer of \( x \) — the set of elements which commute with \( x \).

In the \( \sum_{x \in \Sigma} (G : C(x)) \) term, I'm summing over conjugacy classes with more than one element. This implies two things:

(a) \( (G : C(x)) > 1 \), because \( (G : C(x)) \) equals the number of elements in the conjugacy class.

(b) \( |C(x)| < |G| \), since \( |G| = (G : C(x)) |C(x)| \), and \( (G : C(x)) > 1 \).

**Definition.** Let \( p \) be prime. \( G \) is a \( p \)-group if for all \( g \in G \), \( g \neq 1 \), the order of \( g \) is \( p^n \) for some \( n > 0 \). \( n \) may be different for different elements.

Finite \( p \)-groups are an important class of finite groups. Their structure is described in some detail by **Sylow theory**. Sylow theory is also an important tool in determining the structure of arbitrary finite groups. For example, it provides tools that helps answer questions like: How many different groups of order 20 are there?

As applications of the class equation, I’ll look at some results that are “preliminaries” to Sylow theory.

The first result says that if \( p \) is prime and \( p \mid |G| \), then \( G \) has an element of order \( p \). Note that if \( n \) is not prime, \( n \mid |G| \) does not imply the existence of an element of order \( n \). An easy counterexample: \( |\mathbb{Z}_3 \times \mathbb{Z}_3| = 9 \), which is divisible by 9, but \( \mathbb{Z}_3 \times \mathbb{Z}_3 \) has no elements of order 9.

**Lemma.** Let \( G \) be a finite abelian group, and let \( p \) be a prime number which divides \( |G| \). Then \( G \) has an element of order \( p \).

**Proof.** Induct on \( |G| \). Observe that \( \mathbb{Z}_2 \) has an element of order 2 and \( \mathbb{Z}_3 \) has an element of order 3 (and those are the only groups of order 2 and 3, respectively). This gets the induction started.

Now suppose \( n > 3 \), and assume the result is true for abelian groups of order less than \( n \). Let \( |G| = n \), \( p \mid n \). I want to show that \( G \) has an element of order \( p \).
Let $x \in G$, where $x \neq 0$. If $x$ has order $pk$ for some $k$, then $kx$ has order $p$. Therefore, assume that the order of $x$ is not divisible by $p$.

Now $\langle x \rangle \neq G$, else $x$ has order $n$, and $n$ is divisible by $p$ by assumption. Now

$$p \mid |G| = (G : \langle x \rangle)|\langle x \rangle|.$$ 

Since $p \nmid |\langle x \rangle|$, 

$$p \mid (G : \langle x \rangle) = \frac{|G|}{|\langle x \rangle|}.$$ 

Now $|G/\langle x \rangle| < |G|$ since $|\langle x \rangle| > 1$, so $G/\langle x \rangle$ is an abelian group of order less than $|G|$ whose order is divisible by $p$. By the induction hypothesis, $G/\langle x \rangle$ contains an element $y + \langle x \rangle$ of order $p$, where $y \in G$.

Suppose $y$ has order $m$. Then

$$my = 0, \quad my + \langle x \rangle = \langle x \rangle, \quad m(y + \langle x \rangle) = \langle x \rangle = 0 \in \frac{G}{\langle x \rangle}.$$ 

Since $m$ kills $y + \langle x \rangle$, it follows that $m$ is divisible by the order $p$. Suppose $m = kp$. Then $ky$ has order $p$.

This shows that $G$ has an element of order $p$ and completes the induction.  

**Theorem.** (Cauchy) Let $G$ be a finite group, and let $p$ be a prime number which divides $|G|$. Then $G$ has an element of order $p$.

**Proof.** Induct on $|G|$. Observe that $\mathbb{Z}_2$ has an element of order 2 and $\mathbb{Z}_3$ has an element of order 3 (and those are the only groups of order 2 and 3, respectively). This gets the induction started.

Now suppose $n > 3$, and assume the result is true for groups of order less than $n$. Let $|G| = n$, $p \mid n$. I want to show that $G$ has an element of order $p$.

Consider $x \in \Sigma$, so the conjugacy class of $x$ contains more than one element. By the remarks preceding the lemma, $|C(x)| < |G|$. By induction, if $p \mid |C(x)|$, then $C(x)$ has an element of order $p$. Since $C(x) < G$, I’ll then have an element of order $p$ in $G$.

Therefore, assume that $p \nmid |C(x)|$, for all $x \in \Sigma$. Now

$$p \mid |G| = (G : C(x))|C(x)|.$$ 

Hence, $p \mid (G : C(x))$ for all $x \in \Sigma$. Look at the class equation

$$|G| = |Z(G)| + \sum_{x \in \Sigma} (G : C(x)).$$ 

$p$ divides each term in the summation, and $p$ divides $|G|$ by assumption. Therefore, $p \mid |Z(G)|$. However, $Z(G)$ is an abelian group, so the Lemma shows that it has an element of order $p$. Since $Z(G) < G$, $G$ has an element of order $p$ as well.  

**Corollary.** Let $p$ be prime. The order of a finite $p$-group is $p^n$ for some $n > 0$.

**Proof.** If $G$ is a finite $p$-group, every element has order equal to a power of $p$. If $|G| \neq p^n$ for some $n$, then $q \mid |G|$, where $q$ is a prime number and $q \neq p$. By Cauchy’s theorem, $G$ has an element of order $q$, contradicting the fact that every element of a $p$-group has order equal to a power of $p$. Therefore, $|G| = p^n$ for some $n$.  

**Proposition.** Let $p$ be prime. The center of a nontrivial finite $p$-group is nontrivial.

**Proof.** Examine the class equation

$$|G| = |Z(G)| + \sum_{x \in \Sigma} (G : C(x)).$$
Since \(|G| = p^n|\) for some \(n > 0, p \mid |G|\). If \(x \in \Sigma\), the remarks preceding the lemma above show that \((G : C(x)) > 1\). Since \(p^n = |G| = (G : C(x))|C(x)|\), it follows that \(p \mid (G : C(x))\). Now \(p\) divides \(|G|\) and every term in the summation, so \(p\) divides \(|Z(G)|\). Therefore, \(|Z(G)| \neq 1\). \(\Box\)

**Proposition.** Let \(G\) be a group of order \(p^n\), where \(p\) is prime. Then \(G\) has a subgroup of order \(p^k\) for 

\(0 \leq k \leq n\).

**Proof.** If \(n = 1\), then \(G = \mathbb{Z}_p\), which plainly has subgroups of orders \(p^0\) and \(p^1\).

Assume the result is true for groups of order \(p^{n-1}\), and suppose \(|G| = p^n\). The center \(Z(G)\) of \(G\) is nontrivial; since \(|Z(G)| \mid |G| = p^n\), it follows that \(|Z(G)| = p^j\) for some \(j\). By an earlier result, \(Z(G)\) contains an element \(x\) of order \(p\).

Now \(x \in Z(G)\), so \(\langle x \rangle \subset Z(G)\). Hence, \(\langle x \rangle\) is normal. Form the quotient group \(G/\langle x \rangle\). Now \(|G/\langle x \rangle| = p^{n-1}\), so by induction \(G/\langle x \rangle\) contains subgroups of order \(p^k\) for \(0 \leq k \leq n - 1\). Each such subgroup has the form \(H_k/\langle x \rangle\), where \(H_k\) is a subgroup of \(G\) containing \(\langle x \rangle\).

Suppose then that \(|H_k/\langle x \rangle| = p^k\). I have

\[|H_k| = |H_k/\langle x \rangle| |\langle x \rangle| = p^k \cdot p = p^{k+1}.\]

Thus, \(H_0, H_1, \ldots H_{n-1}\) are subgroups of \(G\) orders \(p, p^2, \ldots p^n\). Obviously, \(G\) contains a trivial subgroup of order \(p^0\). This completes the induction step, and proves the result. \(\Box\)